Office Locations

Boston

Worcester

Springfield

Framingham

Law Offices of

MARK E. SALOMONE

1-800-WIN-WIN-1

Holyoke

Burlington

Roxbury

Ware

Greenfield

August 2, 2010

Attention: Maureen Tobin
Commonwealth of Massachusetts
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Attention: Shannon Choy-Seymour
Commonwealth of Massachusetts
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

RE: 201 CMR 17.00
WISP POLICY SECURITY BREACH MANDATORY REPORT

Dear Ms. Tobin and Ms. Choy-Seymour:

Pursuant to your requests, please be advised of the following in regards to [redacted] file containing personal information being stolen:

1. [redacted] personal information including name, social security number, and driver's license was contained in the stolen file;

2. In addition to immediately notifying [redacted] on July 21, 2010 via a telephone call on the day of the theft, on July 22, 2010 he was given written confirmation of the Lifelock identity protection plan that was purchased in regards to this matter. Additionally, I have forwarded a letter summarizing the events (see attached).

Very truly yours,
Law Offices of Mark E. Salomone

Brigitte V. Freda
Executive Operations Manager – Massachusetts
WISP Security Officer

Enclosure

Office Locations

Boston

Worcester

Springfield

Framingham

Law Offices of

MARK E. SALOMONE

1-800-WIN-WIN-1

Holyoke

Burlington

Roxbury

Ware

Greenfield

August 2, 2010

[redacted]

Dear [redacted]:

This letter is being sent to you to recap the events surrounding the theft of your file from Attorney John J. McQaude's vehicle on July 21, 2010. Attorney McQuade contacted you and spoke with you that same day to immediately inform you that the file was stolen. You then had subsequent conversations with Attorney McQuade on July 22, 2010 to select Lifelock, the identity protection plan of your choice, which the firm had committed to purchase on your behalf. As was discussed, your file was in his vehicle because you and he had attended a deposition. Your file contained what is defined as Personal Information (your name as well as your social security number and driver's license number) in accordance with M.G.L ch 93H.

To date, you are unaware of any issues regarding any consequential issues concerning this theft.

You received written notice on July 22, 2010 regarding the purchase of the identity protection plan and this situation.

Thank you for your attention to this matter.

Very truly yours,
Law Offices of Mark E. Salomone

Brigitte V. Freda
Executive Operations Manager

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
10 Park Plaza – Suite 5170, Boston MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY

July 26, 2010

Brigitte V. Freda
Executive Operations Manager
Law Offices of Mark E. Salmone
175 State Street, Suite 200
Springfield, MA 01103

Dear Ms. Freda:

On July 23, 2010, we recevied a breach notification pursuant to M.G.L.c. 93H, dated July 21, 2010. However, the notification was missing information required by M.G.L.c. 93H. Please either fax, mail or email the following information to us about the breach:

☒ Information breached:
- ☐ Social security number
- ☐ Financial account numbers
- ☐ Driver's license number
- ☐ Debit or credit card numbers

☒ Date notification was made to affected resident:

You may fax it to 617-973-8799 to my attention or email it to me at maureen.tobin@state.ma.us.

Sincerely yours,

Maureen Tobin

Maureen Tobin

There will be no accumulation of vacation time from year to year. Any unused vacation days will be paid out to the employee as a bonus upon request.

WISP PLAN
Written Comprehensive Information Security Program for Records Including Personal Information

In accordance with the Massachusetts Security Breach Notification Law and Data Security Regulations, the Law Offices of Mark E. Salomone strictly follows the below policies and procedures with respect to its client's and employee's *Personal Information*. These policies are designed to prevent identity theft.

Designated Security Officers:

1. Brigitte Freda, Executive Operations Manager
2. John J. McQuade, Managing Attorney
3. Odete Tome-Wells, Pre-Litigations Resources Supervisor
4. Mark W. Bixby, Managing Attorney

As per the Confidentiality Section of this Employee Manual, our client's confidentiality is of the utmost priority for this law firm. This extends to information about a client's case, information contained in our computer database, client documentation, medical records/bills, photographs, related documentation and *Personal Information*.

Personal Information **is comprised of:**
MA residents → **Last name and first name *or***
→ **Last name and first initial**
***AND* one of the following:**
→SS#
→Driver's License #
→MA State Issued ID#
→Financial account, credit card #

1. The preferred method of disposal of any and all documents containing *Personal Information* is to be shredded. Alternatively, documents can also be redacted of all *Personal Information* or burned.

2. Electronic files such as database records, documents, spreadsheets, photographs, etc. must be completed destroyed if discarded and removed from company's hard drive or by completely destroying the hard drive containing *Personal Information.*

3. Files are never to leave the confines of the Law Offices of Mark E. Salomone unless express permission is given by a Security Officer. A file is never to be left in a vehicle or unsecure area and must remain in the employee's reasonable sight and possession.

4. Employee's with laptop computers are not to ever leave said computer in a vehicle or unsecure area. All laptops are to be password protected with unique passwords and must be changed frequently.

5. Examples of Security Breaches:

*Theft of laptop
*Computer hackers
*Intentional accessing of personal information by inappropriate individuals (i.e. must dispose of documents properly
*Poor employee handling of personal information (i.e.: sending e-mail with sensitive info to wrong person or attaching wrong document to e-mail)
*Divulging *Personal Information* contained in the firm contact management software.

Employees are required to report any security breach that they have knowledge of immediately to a Security Officer. Failure to do so subjects said employee to immediate termination.

In the event of a security breach, notice will be sent to the effected party(ies), the Attorney General, and the Director of Office of the Consumer Affairs and Business Regulation (OCABR) as soon as practicable, without unreasonable delay.

In the event of a security breach, it is mandatory that all responsive actions be documented in detail. Additionally, a mandatory post-incident review must take place and an action plan of WISP policy modifications must be implemented within a reasonable period of time.

6. Employee Disciplinary Actions

In the event an employee is found in breach of any of the WISP policies he/she is subject to immediate termination for such willful conduct.

7. Terminated Employees

Once an employee is terminated from employment for any reason, the Law Offices of Mark E. Salomone must take the following steps:

A. Immediately delete their server/network usernames and passwords
B. Immediately have their e-mail account deleted or forwarded to an appropriate staff member.
C. Move the appropriate files under their name in the server to an assigned staff member(s)
D. Delete their alarm codes to the buildings, if applicable.
E. If their keys were not surrendered upon termination, all locks with missing keys are to be changed, if applicable.
F. All voicemail box usernames and passwords are to be removed.
G. Any company owned mobile devices are to be deactivated.
H. In the event of an immediate termination, employee is to be escorted out of the building to prevent any theft of *Personal Information.*

8. Non-Employee/Outsourced Third Party Service Providers

All payroll, accounting, retirement and computer network service providers are to have in place a WISP policy covering these topics to safeguard any client or employee *Personal Information.* Any contracts entered into with these entities must contain a security protection provision.

9. Access to *Personal Information*

   A. Only employee's with a business reason are to access a client or employee's records.
   B. Archive data is kept in secure storage areas in designated office locations.
   C. Employee Personal Information is kept in locked filing cabinets or locked areas at all times under the control of a Security Officer.

10. These policies will be monitored periodically to ensure full compliance. Modifications will be made to the WISP Policies as needed at least annually. Any material change in law firm business practice will necessitate a full review of security practices of procedures.

    All company network hardware containing Personal Information will be protected via a firewall, be monitored for security patch necessity as well as have ongoing and current virus protection software program.

11. Electronic transmission of *Personal Information* via computer transmission must include the following safeguards:

    A. User authentication protocols with secure username and password.
    B. Active accounts are only allowed to transmit data.
    C. No access after multiple unsuccessful attempts to log into a computer device.
    D. Assignment of unique passwords with a reasonable design to maintain data integrity.
    E. Data must be encrypted when sent electronically as attachments.
    F. Data that is faxed from a desktop computer is required to be encrypted. (does not apply to facsimiles, although you must report when a facsimile that contains *Personal Information* is sent to an incorrect recipient)
    G. Data stored on laptops and electronic devices such as smart phones is to be encrypted.

12. New Employees

All new employees will undergo sufficient training in all of these areas to ensure full knowledge and compliance.

The Law Offices of Mark E. Salomone follows the above policies and procedures with respect to *Employee Personal Information* as well.

WORKERS COMPENSATION

The Workers Compensation Law of the Commonwealth of Massachusetts provides that employees sustaining personal injury in the course of their employment be furnished with

Office Locations

Boston

Worcester

Springfield

Framingham

Law Offices of

MARK E. SALOMONE

1-800-WIN-WIN-1

Holyoke

Burlington

Roxbury

Ware

Greenfield

July 21, 2010

Commonwealth of Massachusetts
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Commonwealth of Massachusetts
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

RE: 201 CMR 17.00
WISP POLICY SECURITY BREACH MANDATORY REPORT

Dear Sir or Madam:

Today, I was informed by Attorney John J. McQuade, Jr., an assigned security officer for the firm's WISP policy, that he had a client's file stolen from his vehicle at some point before approximately 6:00 a.m. this morning. The client's file was inside a briefcase that was locked in his trunk inside his locked vehicle in his driveway at his home located at 132 Coventry Lane, Longmeadow, MA. Attorney McQuade reported this incident to the Longmeadow Police Department this morning and to me when I arrived to the office at approximately 9:00 a.m. The reason the file was in the vehicle was it was required for a deposition this week at a location in Worcester, Massachusetts.

The following breach occurred:

1. Attached please see the firm WISP policy which was implemented as part of the Employee Policy Manual effective 2/1/2010;
2. All staff attended a training meeting and signed an acknowledgement of the new policy;
3. In this theft incident, our policy as referenced below was directly violated by employee, John J. McQuade, Jr:

> *Files are never to leave the confines of the Law Offices of Mark E. Salomone unless express permission is given by a Security Officer. A file is never to be left in a vehicle or unsecure area and must remain in the employee's reasonable sight and possession.*

The following actions were taken immediately following the report of this breach:

-the area was searched twice around Mr. McQuade's home and in the general vicinity of the break-in;
-the place where the deposition took place was contacted to see if the file had been left there instead of in the stolen briefcase;

-the employee's home was searched to be sure the file was not located inside the home;
-the client, [redacted] was contacted via telephone to advise his file was stolen which contained his personal information;
-the Law Offices of Mark E. Salomone will purchase an identity theft plan for said client for a period of ten (10) years;
-the Longmeadow police have been contacted repeatedly today and will continue to be contacted to inquire as to whether the file has been found;
-our firm will continue to search for the file in the event that is was inadvertently misplaced elsewhere or if stolen, discarded in an open area;
-the employee/attorney was advised he will be suspended from his employment for two (2) days for violation of the firm WISP POLICY;
-the employee/attorney was advised he has been removed as a security officer of the WISP policy;
-the firm has immediately begun recreating the client's file to ensure this client's case will not be impacted in any way.

Plan of Action to Prevent This from Recurring in the Future:

1. An additional WISP provision which would restrict removing ANY file off site containing personal information. A requirement will be mandated that any personal information will be redacted from files taken offsite for appointments or court proceedings unless required by law.

2. Implement this policy via a meeting and signed acknowledgement from each employee.

Please advise upon your review of this matter of any further recommendations. I will be on vacation from July 26-30, 2010. Should you need to speak to a representative from our firm during that time, please contact our managing attorney, Mark W. Bixby.

Very truly yours,
Law Offices of Mark E. Salomone

Brigitte V. Freda

Brigitte V. Freda
Executive Operations Manager – Massachusetts
WISP Security Officer